UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

UNITED STATES OF AMERICA,

v.

BRIAN LAMONT TURNER,

Defendant.

CASE NO. 3:24-cr-00008

MEMORANDUM OPINION

JUDGE NORMAN K. MOON

The Defendant, Brian Lamont Turner, moves to suppress evidence that the Government obtained from two websites that the Government alleges he used to facilitate sex trafficking and prostitution: (1) Priceline, a hotel reservation site, Dkt. 284, and (2) SkipTheGames, an adult website. Dkt. 285. For the reasons provided below, the Defendant's motions are denied.

I. BACKGROUND

The Defendant contends that federal investigators obtained records from Priceline and SkipTheGames in violation of the Stored Communications Act ("SCA") and the Fourth Amendment. FBI agents requested information from these websites in 2023 while investigating suspected interstate sex trafficking activity. The Defendant – who is now charged with multiple sex trafficking and prostitution-related offenses, Dkt. 297 (Third Superseding Indictment) – challenges the manner in which the Government sought the records. The Court begins by briefly summarizing the investigative conduct at issue.[1]

[1] For the purposes of resolving the motions to suppress, the Court only focuses on conduct related to Priceline and SkipTheGames. The Court's recent opinion addressing the motion to dismiss Count One of the Third Superseding

A. Priceline

Priceline "is an online travel agency that offers discounted rates on travel-related purchases, including flights, hotels, and rental cars." Dkt. 284 at 1.

On July 28, 2023, the Government issued a grand jury subpoena to Priceline. Dkt. 281-1 (Ex. 1) at 1. The subpoena requested records for any accounts associated with certain identifiers – the Defendant's name and date of birth, as well as four email addresses. *Id*. at 3. The subpoena specifically sought subscriber names, addresses, records of all reservations and bookings, contact information for the reservations, and payment information. *Id*.

A supervisor at Priceline emailed FBI Special Agent Mary Echols ("SA Echols") on September 6, 2023 to inform her that the company had no records responsive to the email addresses in the subpoena. Dkt. 284-2 (Ex. 2) at 4. There were too many records associated with the Defendant's name because it is a common name. *Id*. Moreover, Priceline could not narrow the search by birth date. *Id*. Accordingly, the company produced no records but the supervisor informed SA Echols that "[i]f you have any other identifiers, phone numbers or additional email addresses, please let me know and I will try those." *Id*.

SA Echols responded by asking the Priceline supervisor if he could search for two other email addresses and a pair of phone numbers. *Id*. at 3. These identifiers were not listed in the prior subpoena. *Id*. On September 12, 2023, the Priceline supervisor stated in an email that there were also no responsive records based on the new identifiers SA Echols provided. *Id*. at 2. SA Echols replied with a new set of identifiers — four different credit card numbers — for a new query. *Id*. at 1. These were also not in the prior subpoena. *Id*. This time, the Priceline supervisor located responsive records and provided the information in a spreadsheet. *Id*. Priceline

---

indictment provides a more comprehensive overview of the Government's investigation into the Defendant, which started in February 2023. Dkt. 386.

specifically produced records covering October 2021 through August 2023, detailing hotel reservation dates, hotel names, the city and state of each hotel, and the Internet Protocol ("IP") address of the individual making the reservation transaction. *See* Dkt. 284 at 3-4; Dkt. 379 ("May 5, 2025 Hearing Trans.") at 65-66 (Testimony of SA Echols); Dkt. 368, Def. Ex. 17 for May 5, 2025 Hearing (spreadsheet containing the records).[2]

On December 14, 2023, the Government — which now had details about the Defendant's Priceline accounts from the September 2023 records production — issued a new grand jury subpoena to Priceline seeking information associated with two particular email addresses and two specific phone numbers. Dkt. 284-3 (Ex. 3) at 2. This new subpoena sought the same kind of information as the earlier one for the period of "August 28, 2023 through present." *Id*. Priceline subsequently provided responsive records for hotel bookings between July 2023 and January 2024. Dkt. 284 at 4.

The Defendant takes issue with the fact that Priceline produced the first set of records in response to the identifiers provided in SA Echols's emails instead of identifiers set out in a subpoena, court order, or search warrant. Dkt. 284 at 9. He contends this violated the Stored Communications Act and Fourth Amendment. *Id*. at 9-10. Additionally, he argues that the second batch of records was tainted because the subpoena used to request them relied on account information unlawfully obtained through the first set of records. *Id*. at 10.

B. SkipTheGames

SkipTheGames is a website used to arrange sex encounters and escort services. The Defendant quotes from the website's "about" page, which states that it is a site run by people

[2] The spreadsheet itself is not available on the docket, but was uploaded as an Excel document to a Box.com folder for the hearing.

"who believe in privacy, friendliness, and the right for consenting adults to do what they want with each other." Dkt. 285 at 1.

On February 27, 2023, an FBI tactical specialist named Tyler Blevins emailed a representative for SkipTheGames to request that the site provide the email and IP addresses for an account that was "allegedly posting non-consensual ads." Dkt. 285-1 (Ex. 1) at 12. Blevins provided the account name of "Stormy." *Id*. Blevins did not have a subpoena, court order, or search warrant when he requested this information from SkipTheGames.

The representative, Samuel Hanka, replied that he was happy to help but needed more information because the website did not use "account names." *Id*. at 11. Blevins responded by providing a link to an advertisement that had been posted on the site. *Id*.[3] Hanka then provided responsive information – specifically, an email address associated with the post, the sign-up date, and the user's phone number.[4] *Id*. at 9. Hanka emailed Blevins a list of posts that the user had made on the website with the date, time, and IP address of when each post was made. *Id*. at 8-10. Hanka also wrote that the website had the ability to "undelete" posts for Blevins to view but warned that if a user sees prior posts undeleted they may become suspicious. *Id*. at 9.

Shortly after this initial exchange, Blevins sent Hanka a link to a deleted post and asked for information about it because "the deleted post may be a minor and we would like to verify."[5] *Id*. at 8. Hanka said that the post information was already in a file sent to Blevins but he also sent

[3] At a hearing on May 5, 2025, Blevins testified that when he reached out to Hanka, he did not know the identity of the individual depicted in the SkipTheGames post. May 5 Hearing Trans. at 83. He also explained that he did not personally possess information that established the post to be nonconsensual – instead, a database utilized by law enforcement had flagged the post as potentially nonconsensual. *Id*. at 83-84.

[4] The Defendant notes that the Government has associated the email address used for these posts with the Defendant. Dkt. 285 at 2.

[5] Blevins later testified that he did not know the identity of the individual in the post. May 5 Hearing Trans. at 85. A law enforcement database had flagged the post as potentially depicting a minor. *Id*.

links to the photos that appeared in the post. *Id*. Hanka wrote that even when posts are removed, photos that appeared on them remained on the website's server. *Id*.

Another email exchange between Blevins and Hanka in March 2023 show that Hanka provided Blevins with the passwords for two email accounts, including the one referenced above. *Id*. at 1. Hanka also identified other email accounts possibly related to the one associated with the Defendant based on certain photos used by multiple accounts and the device used to authenticate an account. *Id*. at 1-3.

The Defendant states that Hanka provided the Government with "dozens of spreadsheets including data from password-protected SkiptheGames accounts." Dkt. 285 at 3. This included information about the Internet Protocol ("IP") address associated with each post. *Id*.; *see also* Dkt. 285-1 at 10. The Government did not obtain any of the information it received from SkipTheGames with a subpoena, court order, or search warrant. May 5 Hearing Trans. at 79 (Testimony of Tyler Blevins). Like the Priceline records, the Defendant contends the Government obtained SkipTheGames records in violation of the Stored Communications Act and the Fourth Amendment. *Id*. at 3-4.

II. STORED COMMUNICATIONS ACT

A. Legal Standards

The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2713, governs the disclosure of customer communications and records held by certain types of Internet service providers. It applies to two categories of entities, which the statute refers to as "electronic communication service" ("ECS") and "remote computing service" ("RCS") providers.

A provider of an "ECS" offers "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id*. at § 2510(12). A clear example of an ECS is an email system because it allows a user to exchange written communications with other parties. *See Hatley v. Watts*, 917 F.3d 770, 790 (4th Cir. 2019) (explaining that "companies such as Microsoft and Google" function as "electronic communication services when they provide email services through their proprietary web-based email applications," though "that does not mean that Microsoft and Google necessarily function as electronic communication services regarding other applications and services they offer, like cloud-based data processing and analytics services, or goods or products they sell or license, like hardware or software.").

An entity provides an RCS when it is engaged in "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). An example of an RCS is an email service that stores unread messages. *See Hatley*, 917 F.3d at 789.

Section 2703 of the SCA contains provisions that the Government must follow when compelling ECS and RCS providers to turn over user information. Specific requirements regarding the type of process (warrant, court order, or subpoena) turn on the type of provider, the age of the information, and the type of record sought (such as the contents of communications or subscriber information). *See* 18 U.S.C. § 2703(a)-(d).

Section 2707 of the SCA provides several remedies for a party who has been aggrieved by a violation of the Act. These include a civil cause of action in which the party can seek damages, as well as administrative discipline of federal officials who violate the act. *Id*. Significantly, the Act does *not* provide a suppression remedy. *See United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011).

B. Analysis

Applicable Fourth Circuit case law does not precisely define the contours of ECS or RCS outside of the email context. But persuasive authority from other courts underscores that there is an important distinction between (a) websites that provide electronic messaging services, like email providers, or those which offer remote computing, like "cloud" storage services, and (b) those which merely sell products and services through the web. As the parties acknowledge in their briefs, one district court found that the airline JetBlue did not qualify as an ECS provider despite using a website to interact with its customers. The court noted that "a company such as JetBlue does not become an 'electronic communication service' provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers." *In Re JetBlue Airways Corp. Privacy Litigation*, 379 F.Supp.2d 299, 307 (E.D.N.Y. 2005). The court explained that "[a]lthough JetBlue operates a website that receives and transmits data to and from its customers, it is undisputed that it is not the provider of the electronic communication service that allows such data to be transmitted over the Internet. Rather, JetBlue is more appropriately characterized as a provider of air travel services and a *consumer* of electronic communication services." *Id*. (emphasis added). This is consistent with a more generalized finding across cases that "'electronic communication service' encompasses

internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online." *Dyer v. Northwest Airlines Corporations*, 334 F.Supp.2d 1196, 1199 (D.N.D. 2004); *see also Casillas v. Cypress Insurance Co*., 770 Fed Appx. 329, 331 (9th Cir. 2019) (unpublished) ("[W]e have held that websites and services that permit users to communicate directly with one another are considered ECS providers. For instance, an email provider is "undisputedly" an ECS provider."); *Garner v. Amazon.com, Inc.*, 603 F.Supp.3d 985, 1003-04 (W.D. Wash. 2022) ("A company that merely utilizes electronic communications in the conduct of its own business is generally considered a purchaser or user of the communications platform, not the provider of the service to the public."). Similarly, "RCS" has a somewhat technical meaning in the case law. "The statute's legislative history explains that such services exist to provide sophisticated and convenient data processing services to subscribers and customers, such as hospitals and banks, from remote facilities. By supplying the necessary equipment, remote computing services alleviate the need for users of computer technology to process data in-house." *Jetblue,* 379 F.Supp.2d at 310 (citing S.Rep. No. 99–541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564).

Here, Priceline does not come within the ambit of the SCA. Priceline provides a platform that allows customers to make various kinds of travel reservations. That is its main business function. There is no evidence in the record that Priceline allows for user-to-user communication or communication between a user and parties other than Priceline. The Defendant cites to a district court case holding that the short-term home rental website Airbnb was an ECS, *In re United States for an Order Pursuant to 18 U.S.C. § 2705(b)*, 298 F.Supp.3d 201, 210 (D.D.C. 2018), and argues that it is similar to the instant case because Airbnb – like Priceline – is an intermediary between consumers and individual properties. Dkt. 332 at 4. Thus, he urges the

Court to find that Priceline is similarly subject to the SCA. *Id*. Priceline's role as an intermediary may be an accurate description of its business model, but there is nothing in the record about Priceline offering a platform where a user messages directly with another party, like a hotel operator. By contrast, a user-to-user messaging feature provided a key justification for the District Court for the District of Columbia to find that Airbnb qualified as an ECS. *See In re United States for an Order Pursuant to 18 U.S.C. § 2705(b)*, 298 F.Supp.3d at 210 (explaining that "because [short-term rental booking platform] Airbnb's electronic messaging system provides users with the ability to "send or receive wire or electronic communications" to and from each other, 18 U.S.C. § 2510(15), and because all Airbnb users are necessarily users of the messaging system, Airbnb is an ECS provider for the purposes of this matter."). Here, it appears that a user only interfaces with Priceline so that Priceline itself can manage the booking on the customer's behalf. The communications that occur between the user and Priceline are merely incidental to Priceline's business functions. "[J]ust as the use of a telephone to accept telephone reservations does not transform the company into a provider of telephone service," the operation of a website does not transform Priceline into an ECS. *Jetblue*, 379 F.Supp.2d at 307.

Similarly, the record does not establish that Priceline operates as an RCS. An RCS is an entity that participates in "the provision *to the public* of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (emphasis added). While Priceline kept detailed information about prior bookings, such data appear to be internal records that the company kept for its own business purposes. Moreover, based on the limited record related to Priceline, the website does not hold itself out to the public as offering "computer storage or processing services." Indeed, a typical user would probably think they are just using the platform to reserve hotel rooms, rental cars, or flights. It seems highly unlikely a

user would believe they are "storing" or otherwise submitting information to Priceline for purposes akin to placing a document in a "virtual filing cabinet." *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.2d 892, 902 (9th Cir. 2008) (discussing a Senate report on the SCA, S. Rep. No. 99–541 (1986), and noting in a discussion of RCS that "Congress made clear what it meant by 'storage and processing of information.' It provided the following example of storage: 'physicians and hospitals maintain medical files in offsite data banks.' Congress appeared to view 'storage' as a virtual filing cabinet."). While a user can presumably view his own transaction history on the Priceline website, such a feature seems more like a means of simply requesting receipts for the purchase of goods and services than accessing computer storage and processing functions.

Because Priceline is neither an ECS nor an RCS, the SCA is inapplicable to the Priceline information. However, the Court reaches a different conclusion with regard to SkipTheGames.

SkipTheGames is an ECS because users can make posts containing text and images that are aimed at an audience *other than* SkipTheGames itself. This is a key distinction from Priceline, whose customers essentially communicate with the company itself through its website. Moreover, the fact that messages are being sent to an online "bulletin board" accessible to other users, Dkt. 332 at 2, instead of through a private or direct messaging feature between users (similar to email or Airbnb) is not a meaningful difference under the plain text of the ECS definition. Because SkipTheGame provides a platform to distribute what are plainly "electronic communications," it is an ECS. 18 U.S.C. § 2510(12) and (15).

As for RCS status, much of the information SkipTheGames maintained, like login history, IP addresses, and verification photos, are internal company records that were not generally accessible to the public. However, it appears that users have access to some storage

functions on the website. In an email to Blevins, Hanka described a "scheduling" feature through which a user may schedule a post hours or days in advance. Dkt. 285-1 at 6. The record is not entirely clear on how this function works, but the existence of a scheduling function presumably means that users could "store" certain communications for future distribution. This fits within the definition of an RCS because it involves the retention of communications for later use or access, like a stored email system.

Nevertheless, there are two significant barriers to the relief that the Defendant seeks.

First, some of the SkipTheGames-related information cannot form the basis for an SCA violation. As the Government correctly notes, Dkt. 321 at 11, the Wiretap Act - a different, but related statute – specifically provides that "[i]t shall not be unlawful under this chapter or [the SCA] for any person … to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). The Defendant makes much of the fact that many of the posts SkipTheGames gave to law enforcement were previously deleted and thus no longer accessible to the public. Dkt. 332 at 2. But that is a distinction without a difference because the posts were publicly available at one point or another. Anyone could have viewed these posts at the time they were made.[6]

Second, the SCA does not provide suppression as a remedy for violations of the relevant provisions. Thus, even if the Court assumes without deciding that the Government violated the SCA by obtaining information from SkipTheGames through informal email contact instead of a

[6] Indeed, it appears that the Government was aware of some of the posts in real-time. Blevins testified about a database tool that the Government used to flag posts as possibly depicting minors and nonconsensual content. May 5, 2025 Hearing Trans. at 81-88. It appears that in at least one instance, the database identified a post as featuring a potential minor prior to the post's deletion. *Id*. at 85-86 (describing post at issue in an email exchange on February 28, 2023); *see also* Dkt. 285-1 at 8 (copy of email exchange).

subpoena or other formal process, it lacks the statutory authority to suppress the evidence at issue.

As noted earlier, Section 2707 of the SCA provides several remedies – including a civil cause of action – for a party who has been aggrieved by a violation of the Act. But the Act expressly provides that "[t]he remedies and sanctions described in this chapter are *the only* judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708 (emphasis added). Because the Act does not supply suppression as a remedy or sanction, it is unavailable here. *See United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011) ("Congress has shown that it knows how to create a statutory suppression remedy. It did so in 18 U.S.C. § 2515, which provides for suppression of evidence obtained in violation of the statutes governing wiretaps. Yet it chose not to do so in the context of § 2703(c) violations. Therefore, *Congress has made clear that it did not intend to suppress evidence gathered as a result of § 2703(c) violations."*) (emphasis added); *see also United States v. Karmo*, 109 F.4th 991, 994 (7th Cir. 2024) ("Even if Karmo could prove a violation of the Stored Communications Act, suppression of evidence is not an available remedy."); *United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014) ("[S]uppression is not a remedy for a violation of the Stored Communications Act."). Accordingly, the Court must deny the Defendant's motions to the extent he seeks to suppress evidence on the grounds of alleged SCA violations.

Of course, suppression *is* an available remedy for violations of an individual's constitutional rights. Thus, the Court must also consider whether the Government violated the Fourth Amendment when it obtained the information from Priceline and SkipTheGames without a warrant.

III. FOURTH AMENDMENT

A. Legal Standards

The Fourth Amendment prohibits "unreasonable searches and seizures." U.S. Const. amend. IV. To protect this right, courts utilize the exclusionary rule, which dictates that "evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure." *United States v. Calandra*, 414 U.S. 338, 347–48 (1974).

The Defendant contends that the evidence at issue in his motions was obtained through unlawful searches of the Priceline and SkipTheGames accounts. Dkts. 284-85. Thus, the threshold question here is whether the alleged searches implicate the Fourth Amendment. As the Fourth Circuit has explained, "a search occurs for constitutional purposes only 'when an expectation of privacy that society is prepared to consider reasonable is infringed.'" *United States v. Stephens*, 764 F.3d 327, 331 (4th Cir. 2014) (citations omitted). Accordingly, "[o]fficial conduct that does not compromise any legitimate interest in privacy is not a search subject to the Fourth Amendment." *Id.* (citations omitted). "'In order to demonstrate a legitimate expectation of privacy, [a defendant] must have a subjective expectation of privacy,' and that subjective expectation of privacy must be 'objectively reasonable; in other words, it must be an expectation that society is willing to recognize as reasonable.'" *United States v. Castellanos*, 716 F.3d 828, 832 (4th Cir. 2013) (citations omitted).

Related to this analysis is the "third-party doctrine," whereby an individual generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). This doctrine originated in cases involving law enforcement's collection of bank and telephone company records. *See id*. at 741-

46; *United States v. Miller*, 425 U.S. 435, 440-43 (1976). In *Miller*, the Supreme Court explained that it "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id*. at 443. The third-party doctrine, however, has some important limits. Relevant to the Defendant's arguments in the instant motions is that in *Carpenter v. United States*, the Supreme Court declined to extend the third-party doctrine to cell site location information ("CSLI"). 585 U.S. 296, 309-10 (2018). The *Carpenter* decision acknowledged that while cell phone location records "are generated for commercial purposes," such records merited Fourth Amendment protection (i.e., require a warrant supported by probable cause) because of their "unique nature." *Id*. at 309, 311. More specifically, the Court explained that an individual has a "reasonable expectation of privacy in the whole of his physical movements" and CSLI implicates this privacy interest because it provides a comprehensive, "detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id*. at 313-15.

B. Analysis

Even assuming that the Defendant demonstrated a subjective expectation of privacy in the Priceline booking information and the SkipTheGames records by using a password for his accounts,[7] Dkt. 284 at 12-13, Dkt. 332 at 6-7, the Court is not persuaded that he has a reasonable privacy interest in any of these records.

[7] The Defendant cites to *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) for the proposition that password-protected records enjoy Fourth Amendment protections because the user has demonstrated an intent to exclude others from the information. Dkt. 284 at 12-13; Dkt. 332 at 6. This may be true as a general observation about passwords, but the Defendant does not sufficiently grapple with how security features like user passwords intersect

As an initial matter, it is hard to see how there is any reasonable expectation of privacy in the content of SkipTheGames posts that were made to a public audience. This is not a case, for example, where an individual posted content to a website with the intent that it only be viewed by his chosen circle of friends. *See, e.g., United States v. Chavez*, 423 F.Supp. 3d 194, 201-05 (W.D.N.C. 2019) (concluding that a defendant who limited access to certain content on his Facebook profile to "Facebook Friends" had "manifested a subjective expectation of privacy in his *non-public* Facebook content that society is prepared to recognize as reasonable.") (italics added). As far as the Court can tell from the limited record, the SkipTheGames posts were visible to *anyone* on the website. Even the deleted posts were, presumably, previously accessible to everyone accessing the website. The public nature of these posts undercuts his ability to now assert a Fourth Amendment privacy interest in them. *See Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection.").

The Priceline and SkipTheGames records also both squarely fall under the third-party doctrine.

The information that the Defendant conveyed to the Priceline website to secure hotel reservations are "business records" like the bank records in *Miller*. 425 U.S. at 440. As the *Miller*

---

with the third-party doctrine. Much of the information that people convey to third parties has security protections but that does not change how a person has a reduced privacy interest when they voluntarily convey information to a third party as part of their access to the third party's services. Additionally, *Trulock* involved two individuals who lived at the same residence and shared a common computer but used individual passwords to protect their own files. Each user had a reasonable expectation in the privacy in their own files and did not have authority to consent to the search of the other's files. 275 F.3d at 403. ("By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. Moreover, because he concealed his password from Conrad, it cannot be said that Trulock assumed the risk that Conrad would permit others to search his files. Thus, Trulock had a reasonable expectation of privacy in the password-protected computer files and Conrad's authority to consent to the search did not extend to them. Trulock, therefore, has alleged a violation of his Fourth Amendment rights."). Here, however, the Defendant did not hide his information from either Priceline or SkipTheGames. He affirmatively provided it to them as part of his use of their services. Thus, he did not withhold his information from either platform in a manner analogous to an individual who uses a password to hide his files from a co-user of his computer.

Court observed, "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id*. at 442. Similarly, the Priceline records contain basic information that one would expect a travel reservation company to obtain for each reservation – that is, the hotel location, number of rooms, and details about the person who booked the room. Dkt. 368, Def. Ex. 17 for May 5, 2025 Hearing (spreadsheet containing the records). The Defendant voluntarily conveyed this information to Priceline and assumed the risk that "in revealing his affairs to another … information will be conveyed by that person to the Government." *Miller*, 425 U.S. at 443; *see also Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.")

Similarly, the SkipTheGames account information is a standard business record. To access the website's services, a user provides some personal information like an email and phone number. As the Fourth Circuit has explained both before and after *Carpenter*, a user has no reasonable expectation of privacy in such subscriber information. *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (applying third-party doctrine to subscriber information – "name, email address, telephone number, and physical address" – and holding that even if the defendant "could show that he had a subjective expectation of privacy in his subscriber information, such an expectation would not be objectively reasonable."); *United States v. Wellbeloved-Stone*, 777 Fed. Appx. 605, 607 (4th Cir. 2019) (per curiam) (unpublished) (applying *Bynum* to hold that a defendant "had no reasonable expectation of privacy in his subscriber information, and the Government did not perform a Fourth Amendment search by obtaining that information."). Thus,

as with the Priceline records, basic user information voluntarily conveyed to SkipTheGames came with "the risk that the information would be divulged to police." *Smith*, 442 U.S. at 745.

The Defendant suggests that the third-party doctrine is not applicable to the SkipTheGames records because at least some of them, like the posts, "are not records that were created, owned, or controlled by SkipTheGames." Dkt. 332 at 6. The records in *Miller* and *Smith*, by contrast, "were created, owned, and controlled by the companies." *Id*. This is not a convincing distinction because SkipTheGames does, in fact, create and control comprehensive records of accounts and the content posted on its site – and for good reason. Although the record does not reveal a user agreement or language that an individual consents to when creating a SkipTheGames account, the very nature of a website that contains adult material suggests that the platform has an interest in monitoring postings to ensure that certain content – such as child exploitation or other non-consensual material – is not posted. Thus, it is unsurprising that SkipTheGames's "about" page — which the Defendant cites in his motion to suppress, Dkt. 285 at 1 — expressly advises users that it will readily comply with law enforcement requests because it does not wish to be associated with non-consensual activity.[8] *See About*, SkipTheGames, https://skipthegames.com/about (last accessed July 14, 2025). This disclaimer is consistent with the statements that appear in Hanka's email exchanges with Blevins. *See* Dkt. 285-1 at 5, 7-9, 11

[8] The "about" page specifically states as follows:

> [I]n order to use this site you have to be an adult and you have to be consenting.
>
> If you work with law enforcement and you are investigating something non-consensual that is related to our site, or involves a minor, please contact us. You do not need a subpoena or a court order, because honestly, fuck those people who do things like that.
>
> You may ask about the rights and privacy of people, and where do you draw the line? We say, well, it is our site, and we'll draw it on the other side of people like that."

About, SkipTheGames, https://skipthegames.com/about (last accessed July 14, 2025).

(email signature for Hanka, stating in bolded text, "We have a strict no minors and no non-consensual activity policy.") While the Court finds that the public posts lack Fourth Amendment protections, *supra* at 15, the website's obvious concern with deterring certain kinds of illegal activity supports the conclusion that its documentation of prior posts are also business records that one would understandably expect a sexually explicit adult platform to create in the "ordinary course of business." The fact that a SkipTheGames user places some sort of "confidence" in the site for the "limited purpose" of posting a public sex ad does not give the user complete control over the content because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443.

To be sure, both Priceline and SkipTheGames collected some location-related information. Specifically, both sites collected IP addresses. Dkt. 368, Def. Exs. 10 and 17 for May 5, 2025 Hearing (spreadsheets containing SkipTheGames and Priceline records).[9] The Priceline records also identified hotels where the Defendant booked rooms. *Id*. at Def. Ex. 17. The Defendant suggests that this kind of information enables the kind of monitoring of physical movement that requires a warrant under *Carpenter*. Dkt. 284 at 14-15; Dkt. 285 at 7-8; Dkt. 332 at 7. But the *Carpenter* decision involved location data that is meaningfully distinct from the records at issue here.

Carpenter emphasized the involuntary nature of CSLI. The decision explained that one of the rationales for the third-party doctrine – "voluntary exposure" – was inapplicable because "[c]ell phone location information is not truly 'shared' as one normally understands the term." 585 U.S. at 315. The Court noted that a cell phone is a "pervasive … part of daily life" and that it

[9] Like the Priceline spreadsheet, the spreadsheet of SkipTheGames posts was uploaded to a Box.com folder for the May 5, 2025 hearing.

"logs a cell-site record by dint of its operation, *without any affirmative act on the part of the user* beyond powering up." *Id*. (emphasis added); *see also id*. ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates.") Thus, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id*. By contrast, the data at issue here requires a user to affirmatively decide to use Priceline or SkipTheGames. The Defendant specifically contends that IP information gathered by a website is not voluntary because such data "is logged simply through the accessing of the website with no affirmative act by the user beyond logging in." Dkt. 332 at 7. This argument fails to appreciate that "logging in" *is* a significant voluntary act. The data is only available because the Defendant voluntarily visited and utilized the websites' services. Since *Carpenter*, several federal courts have similarly recognized the voluntariness of sharing IP address data. *See United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) ("[A]n internet user generates the IP address data … only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in *Carpenter*, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger.); *United States v. Brooks*, 841 Fed. Appx. 346, 350 (3d Cir. 2020) (noting that that "there is no reasonable expectation of privacy in subscriber information," like IP addresses, "voluntarily conveyed to third parties"); *United States v. Soybel*, 13 F.4th 584, 593 (7th Cir. 2021) (distinguishing *Carpenter* and rejecting that a defendant's IP address data was created without any affirmative act beyond turning on a device). Fourth Circuit case law has not provided a reason to break with these persuasive precedents.

Additionally, the sheer quantity of location data and the precision of CSLI is distinct from that of hotel information and IP addresses, which only offer limited insights into a person's physical location. In *Carpenter*, the Government obtained 127 days of cell-site data, including "12,898 location points" or "an average of 101 data points per day." 585 U.S. at 302. The Court explained that CSLI "is rapidly approaching GPS-level precision" and "with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters." *Id*. at 313. Given the pervasiveness of cell phones in daily life, the Court observed that "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id*. at 312-13.

A record of where an individual booked a hotel room only reveals where the individual may have spent the night (and, as the Government points out, an individual who books a hotel room may not necessarily be the same person who stays in the room, Dkt. 321 at 8). A reservation record certainly does not enable anywhere near the same level of surveillance akin to "an ankle monitor." *Carpenter*, 585 U.S. at 312. While this type of record documents one place that a person may have been on a particular date, it provides no other details about an individual's whereabouts such as where else he traveled while staying at the hotel. CSLI, on the other hand, offers a far more "detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Carpenter*, 585 U.S. at 315.

IP addresses similarly disclose limited location information. An IP address "is a string of characters associated in an internet provider's business records with a particular device connecting to the internet through a particular network." *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020). IP information "can be translated into location information only indirectly,

by examining the internet company's business records to determine the physical address where the network is registered." *Id.*; *see also Hood*, 920 F.3d at 92 (stating that the IP address data that the government acquired from a smartphone messaging application "does not itself convey any location information."); *United Stats v. Zhou*, 2025 WL 218831, at *5-6 (E.D.N.Y. Jan. 16, 2025) (noting that "IP addresses are the type of 'business records that might incidentally reveal location information' that *Carpenter* explicitly did not disturb." (quoting *Carpenter*, 585 U.S. at 316)). Admittedly, the record here is not entirely clear about how the Government transformed IP addresses into approximate locations. *See, e.g.*, Dkt. 285 at 7 (excerpt of search warrant affidavit referring to June 2023 advertisements on SkipTheGames for Charlottesville and Lynchburg "from an IP address that resolves back to Lynchburg, Virginia"). However, there is no evidence that IP address data generates precise, geographically accurate information that enables "near perfect surveillance" like CSLI does. *Carpenter*, 585 U.S. at 312. Indeed, at oral argument, defense counsel seemed to acknowledge the limitations of IP address data: "They [the Government] use that information to show that the post was made in Greensboro. Now, from the evidence we've been provided so far in discovery it doesn't get more specific, oftentimes get more to a very specific exact location." May 5, 2025 Hearing Trans. at 100-01. As the Court understands it, the IP addresses can essentially be used to show the date and time that a device accessed a website in a particular locale, but it does not create an "all-compassing record" of an individual's exact location and physical movements. *Carpenter*, 585 U.S. at 311. This is further underscored by the small number of individual data points that the Government received. In *Carpenter*, the CSLI consisted of a daily average of 101 data points. Here, the Priceline spreadsheet features 643 reservations between October 16, 2021 and August 28, 2023 (a period of 681 days). Because each reservation included an IP address, this amounts to about just one IP

address data point per day. Dkt. 368, Def. Ex. 17 for May 5, 2025 Hearing (spreadsheet containing the records). As for the SkipTheGames posts, a spreadsheet introduced at the May 5 hearing captured 675 posts between December 19, 2022 and March 16, 2023 (87 days). Each post is associated with an IP address, and each post that was deleted – 648 of the posts – also has an IP address for the "deleter." This breaks down to an average of about 15 IP addresses per day (1,323 IP address data points across 87 days). As another court noted when conducting a similar analysis of IP addresses, "[t]hat the records here provided significantly fewer data points each day [than in *Carpenter*] strongly suggests" that the IP address logs at issue "do not 'give the Government near perfect surveillance' in a manner similar to CSLI, GPS-trackers, or ankle monitors." *United States v. Hernandez*, 2020 WL 3257937, at *20 (S.D.N.Y. June 16, 2020).

648

Given the above observations, the Defendant has failed to show that *Carpenter* required the Government to secure a warrant before obtaining the Priceline and SkipTheGames data. This is consistent with the Fourth Circuit's holding in a post-*Carpenter* (albeit unpublished) decision holding that a defendant "had no reasonable expectation of privacy in his IP address or subscriber information." *Wellbeloved-Stone*, 777 Fex. Appx. at 607. As the Supreme Court emphasized in *Carpenter*, its decision was "narrow." 585 U.S. at 316. The Court left much of the third-party doctrine intact. Indeed, it did not "address other business records that might incidentally reveal location information," *id*. at 316, which are the kind of records at issue here. The information produced by these websites simply does not resemble "the exhaustive chronicle of location information casually collected by wireless carriers today." *Id*. at 314.

In sum, the Defendant did not have an objectively reasonable expectation of privacy in the Priceline and SkipTheGame records. The third-party doctrine, as well as the public-facing

nature of the SkipTheGames posts, leads to this conclusion. Thus, a warrant was not required for the Government to obtain these records.

CONCLUSION

For the reasons provided above, the Defendant's motions to suppress the Priceline and SkipTheGames records, Dkts. 284 and 285, will be **DENIED** in an accompanying order entered on this date.

Entered this 15th day of July, 2025.

NORMAN K. MOON
SENIOR UNITED STATES DISTRICT JUDGE